INVESTIGATING THE RELATIONS OF ATTACKS, METHODS AND OBJECTS IN REGARD TO INFORMATION SECURITY IN NETWORK TCP/IP ENVIRONMENT

Dimitrina Polimirova, Eugene Nickolov, Cecko Nikolov

Abstract: Possibilities for investigations of 43 varieties of file formats (objects), joined in 10 groups; 89 information attacks, joined in 33 groups and 73 methods of compression, joined in 10 groups are described in the paper. Experimental, expert, possible and real relations between attacks' groups, method' groups and objects' groups are determined by means of matrix transformations and the respective maximum and potential sets are defined. At the end assessments and conclusions for future investigation are proposed.

Keywords: File Formats, Information Attacks, Methods of Compression, Compressed Objects, Information Security.

ACM Classification Keywords: D.4.6 Security and Protection: information flow controls

The Situation

The new technologies' development extends the necessity of processing, transferring and saving of volume sizable information flows. These information flows, in the form of file objects, are an object of non-stop attacks according to their information security, which determines the significant necessity for investigation of methods and means for their protection.

Researches are carried out in two directions. The first one is connected with the development of different and new techniques for decreasing the volume of information flows (for example: different methods of compression). The other one is connected with the possibility of increasing the safety of their information security with respect to different attacks.

The Problem

A general strategy for protecting file objects could include applying compression methods to objects to achieve simultaneously decrease in volume size of information flow and increase its information security with respect to different kinds of attacks, which it can be exposed on. In additional the use of password with fixed minimum and maximum length can be used. The possibility for encryption of objects, which are preliminarily compressed and protected by password, can be included as the last stage of the strategy for protecting. The main parameter to this stage is the length of applied key.

For the purposes of the investigation the following reservation can be made: it is enough to investigate only the influence of compression methods on objects exposed to one or more attacks, as the difference in their behavior before and after the attacks when standard and not corporate (government) requirements are used is taken into consideration.

The Experiment

The experiment which is carried out is connected to objects, exposed to information attacks and processed by methods of compression to increase their information security.

To achieve the end of this investigation it is necessary to determine the sets of ATTACKS, METHODS and OBJECTS, which will take part in the experiments for determining the information security. With regard to this investigation the following tasks were posed:

1) To determine the *SETS OF MAXIMUM* attacks, methods of compression and objects.

The set of all attacks, known by now, has to be determined. They will form the set of maximum number of attacks (A_{max}), which can be collected from the current information base of National Laboratory of Computer Virology of Bulgarian Academic of Sciences. It collects information for the information attacks, which were carried out to a

separate personal and/or corporate computers, and/or networks, and/or systems at the moment of the investigation. 89 different attacks will be analyzed [1]. This is a generalization of attacks, implemented in Bulgaria, Balkan Peninsula and south-east Europe. The attacks have been provisionally divided into malware and malattacks. In case of malware the direct participation of a user at the moment of the attack is missing, while in case of malattack the user's presence is required. Varieties, known for this period, are organized in 33 groups, respectively 20 for malware and 13 for malattack. To achieve calculative expenses reducing and visualization improving, conclusions on the base only of 33^{th} groups not for 89^{th} varieties are described below after experiments which were carried out.

For the purposes of the investigation, the current attacks will be denoted as a_i, where the index *i* changes from 1 to *n* (maximum number of known attacks).

The maximum numbers of objects (O_{max}), which will be described, are different kinds of file formats. We shell understand as file format the specific organization of information within a file [2]. Different types of file formats exist for the different type of information. They are separated in 43 varieties, which will be called only *objects*, joined in 10 main groups. During the experiments the different file formats will be represented by different file extensions. (Over 18000 file extensions are known at the moment [3]). To achieve calculative expenses reducing and visualization improving, conclusions on the base only of 10^{-th} groups not for 43^{-th} varieties are described below after experiments which were carried out.

For the purposes of the investigation, the current object will be denoted as o_f, where the index *f* changes from 1 to *l* (maximum number of objects).

Different kinds of compression methods will be selected for protecting the objects exposed to attacks. They will create the set of maximum number of methods (M_{max}), called only *methods*. Seventy three methods in 10 groups will be analyzed. Five of them are assigned to lossless methods of compression and the other five to lossy methods of compression [4]. To achieve calculative expenses reducing and visualization improving, conclusions on the base only of 10^{-th} groups not for 73^{-th} varieties are described below after experiments which were carried out.

For the purposes of the investigation, the current method of compression will be denoted as m_j, where the index *j* changes from 1 to *k* (maximum number of methods).

2) To determine the ***SETS*** *of POTENTIAL* attacks, methods and objects, which will take a part in the experiments.

The attacks, methods and objects having direct relation to the investigation and forming the sets of potential attacks, methods and objects have been singled out.

To turn out the unreal relations from the determined maximum sets, attacks, methods and objects have to be singled out by reducing. They will form the sets of potential attacks, methods and objects.

To determine the potential attacks, methods and objects, matrices have been devised with the results of *expert* assessment and *experiments* on the relations attack-object, method-object and attack-method. The results will provide the possibility to exclude from the analysis the attacks, methods and objects about which: 1) there is no sufficient information; 2) the information is not public; 3) the information is rapidly changing; 4) there is not enough authentic hardware and software.

The expertly determined sets of relations will be put to a partial test by means of a number of planned simulative experiments. Thus the set of possible attacks, methods and objects will be singled out and: 1) the possible attacks are expertly and experimentally estimated for the relevant object/objects in connection with relevant method/methods; 2) the possible methods are expertly and experimentally estimated for the relevant object/objects in connection with relevant attack/attacks; 3) the possible objects are expertly and experimentally estimated for the relevant method/methods in connection with relevant attack/attacks.

2.1.) To determine the *POSSIBLE RELATIONS* attack-object, method-object and attack-method.

Determination of *possible* relations attack—object (Ω)

Two matrices are composed to determine the set Ω: $E_{(l,n)}$ and $Y_{(l,n)}$. By the vertical of the matrices are included all attacks A_{max}, separated in n varieties $a_1, a_2,\ldots, a_i,\ldots,a_n$, $\bigcup_{i=1}^{n} a_i = A_{\max}$, $\bigcap_{i=1}^{n} a_i = \varnothing$. By the horizontal of the matrices are included all objects O_{max}, separated in l varieties $o_1, o_2,\ldots, o_f,\ldots,o_l$, $\bigcup_{f=1}^{l} o_f = O_{\max}$, $\bigcap_{f=1}^{l} o_f = \varnothing$. A research is conducted, where an attack a_i is trying to get access ρ to the object o_f, where ρ will present the different type of an access (read, write, execute and delete). Graphically this process can be illustrated in this way:

$$U_1 \longrightarrow a_i \xrightarrow{\rho} o_f$$

where U_1 is a user, who uses an attack $a_i \subseteq A_{max}$, to get access ρ to the object $o_f \subseteq O_{max}$, $i=1,2,\ldots,n$, $f=1,2,\ldots,l$.

In the first matrix $E_{(l,n)}$ for each cell a logical processing is made with result logical 0 or logical 1 by the so called function of truth [5] $I_x(B)\begin{cases}1, x \in B\\ 0, x \notin B\end{cases}$ respectively for the attack and object: $I_a(a_1), I_a(a_2),\ldots, I_a(a_i),\ldots, I_a(a_n)$, $I_o(o_1), I_o(o_2),\ldots, I_o(o_f),\ldots, I_o(o_l)$ and in the corresponding cell of the matrix is filled out the result from the logical expression: $I_a(a_i) \wedge I_o(o_f)$ on the of the experiments, which were carried out. If the obtained result is 1 (possible) ($x=1$) then during the experiments the attack had gotten an access to the object ($A \xrightarrow{\rho} O$), otherwise with result 0 (impossible) ($x=0$), the attack's access is not accomplished. On the base of the obtained results the set F can be singled out, which include all attacks and objects, for which is completed the following condition: $I_a(a_i) \wedge I_o(o_f) = 1$.

In the second matrix $Y_{(l,n)}$ for each cell the function of truth is produced on the base of expert assessments: $Y_x(K)\begin{cases}1, x \in K\\ 0, x \notin K\end{cases}$ for the attack and object: $Y_a(a_1), Y_a(a_2),\ldots, Y_a(a_y),\ldots, Y_a(a_n)$, $Y_o(o_1), Y_o(o_2),\ldots, Y_o(o_f),\ldots, Y_o(o_l)$. For each oriented graph $A \xrightarrow{\rho} O$ the result from the following logical expression $Y_a(a_i) \wedge Y_o(o_f)$ is filled out. If the obtained result is 1 (true) ($x=1$), then an attack A can get access to the object O ($A \xrightarrow{\rho} O$), otherwise with result 0 ($x=0$), the attack A can not get an access ρ to the object O. From the obtained results the set E can be singled out, which includes all attacks and objects the following logical expression is realized for: $Y_a(a_i) \wedge Y_o(o_f) = 1$.

Crossing the set F with E ($F \cap E$) the set of possible relations attack—object (Ω) can be singled out, where $\Omega = \left[I_a(a_i) \wedge I_o(o_f) \right] \wedge \left[Y_a(a_i) \wedge Y_o(o_f) \right] = 1$. On Figure 1 are graphically presented the obtained result for possible relations between attacks' groups and objects' groups. To achieve calculation expenses reducing and visualization improving is working only with groups.

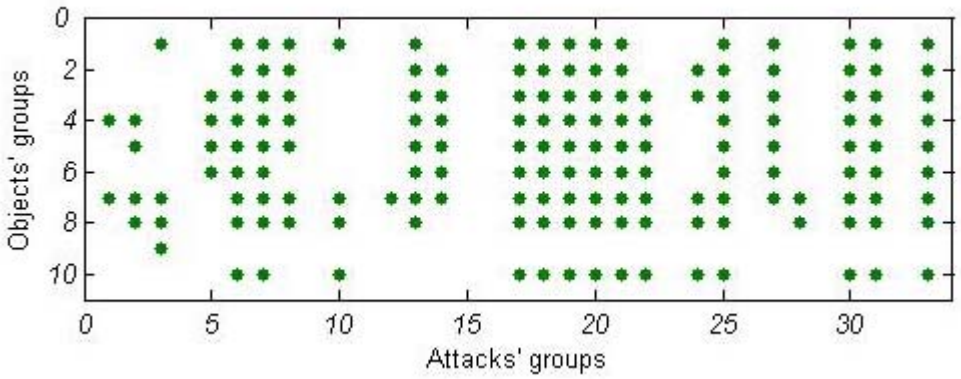

Figure 1 Possible relations between attacks' groups and objects' groups

Determination of *possible* relations method—object (Ξ)

Two matrices are composed to determine the set Ξ: $E_{(l,k)}$ and $Y_{(l,k)}$. By the vertical of the matrices are included all methods of compression M_{max}, separated in k varieties $m_1,m_2,\ldots,m_j,\ldots,m_k$, $\bigcup_{j=1}^{k} m_j = M_{\max}$, $\bigcap_{j=1}^{k} m_j = \varnothing$. By the horizontal are included all objects O_{max}, separated in l varieties $o_1, o_2,\ldots, o_f,\ldots,o_l$, $\bigcup_{f=1}^{l} o_f = O_{\max}$, $\bigcap_{f=1}^{l} o_f = \varnothing$. A research is conducted, where each object is processes by each methods of compression. Graphically this process can be illustrated by this way:

$$U_2 \longrightarrow m_j \longrightarrow o_f$$

where U_2 is a user, who processes the object $o_f \subseteq O_{max}$ with methods of compression $m_j \subseteq M_{max}$, $f=1,\ldots,l$, $j=1,\ldots,k$.

For each cell of the matrix $E_{(l,k)}$ a logical processing is made with result logical 0 or logical 1 by the so called function of truth: $I_x(B)\begin{cases}1, x \in B\\ 0, x \notin B\end{cases}$ for the methods and object: $I_m(m_1),I_m(m_2),\ldots,I_m(m_j),\ldots, I_m(m_k)$, $I_o(o_1),I_o(o_2),\ldots,I_o(o_f),\ldots,I_o(o_l)$ and in the corresponding cell of the matrix is filled out the result from the logical expression: $I_m(m_j) \wedge I_o(o_f)$ on the of the experiments, which were carried out. If the obtained result is 1 (possible) ($x=1$), then during the experiment the method has successfully applied to the object ($M \longrightarrow O$), otherwise with result 0 (impossible) ($x=0$), during the experiment the method has not successfully applied to the object. On the base of the obtained results the set C can be singled out, which include all methods and objects, for which is completed the following condition: $\mathrm{I}_m\left(m_j\right) \wedge I_o\left(o_f\right) = 1$.

For each cell from the second matrix $Y_{(l,k)}$ the function of truth is produced on the base of expert assessments: $Y_x(K)\begin{cases}1, x \in K\\ 0, x \notin K\end{cases}$ for the method and object: $Y_m(m_1),Y_m(m_2),\ldots,Y_m(m_j),\ldots,Y_m(m_k)$, $Y_o(o_1),Y_o(o_2),\ldots,Y_o(o_f),\ldots,Y_o(o_l)$. For each oriented graph $M \longrightarrow O$ the result from the following logical expression $Y_m(m_j) \wedge Y_o(o_f)$ is filled out. If the obtained result is 1 (true) ($x=1$), then method M can be applied to object O ($M \longrightarrow O$), otherwise with result 0 ($x=0$), a method M can not be applied to an object O. From the obtained results the set P can be singled out, which include all methods and objects, the following logical expression is realized for: $Y_m(m_j) \wedge Y_o(o_f) = 1$.

Crossing the set *C* with *P* ($C \bigcap P$) the set of possible relations method—object (Ξ) can be singled out, where $\Xi = \left[I_m\left(m_j\right) \wedge I_o\left(o_f\right) \right] \wedge \left[Y_m\left(m_j\right) \wedge Y_o\left(o_f\right) \right] = 1$. On Figure 2 are graphically presented the obtained results for possible relations between methods' groups and objects' groups. To achieve calculation expenses reducing and visualization improving is working only with groups.

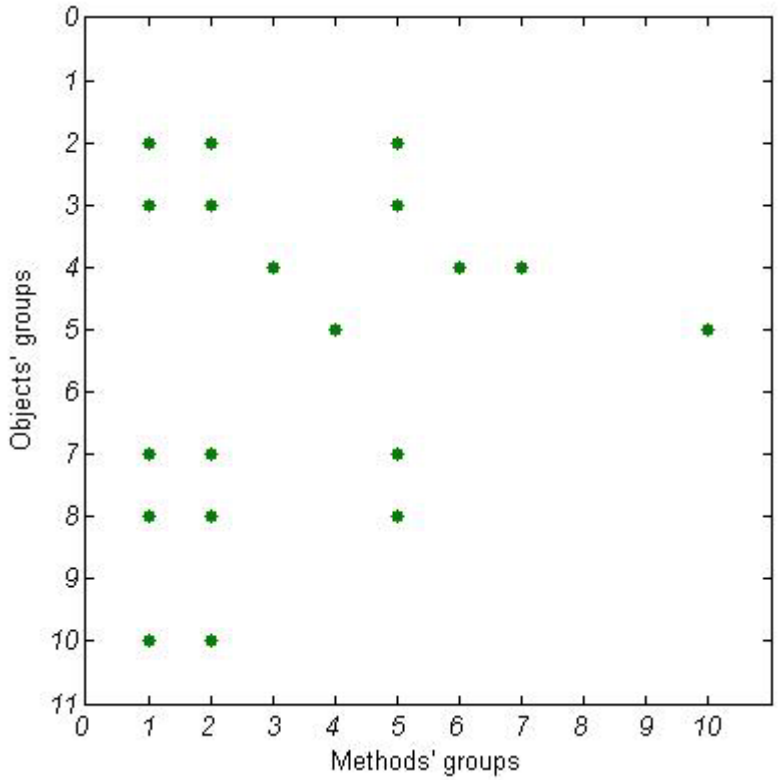

Figure 2 Possible relations between methods' groups and objects' groups

(Methods groups 8 and 9 were dropped out from the investigation after expert assessment.)

Determination of *possible* relations attack—method (Θ)

Two matrices are composed to determine the set Θ: $E_{(k,n)}$ and $Y_{(k,n)}$. By the vertical of the matrices are included all attacks A_{max}, separated in *n* varieties $a_1,a_2,\ldots,a_i,\ldots,a_n$, $\bigcup_{i=1}^{n} a_i = A_{\max}$, $\bigcap_{i=1}^{n} a_i = \varnothing$. By the horizontal are included all methods of compression M_{max}, separated in *k* varieties $m_1,m_2,\ldots,m_j,\ldots,m_k$, $\bigcup_{j=1}^{k} m_j = M_{\max}$, $\bigcap_{j=1}^{k} m_j = \varnothing$. A research is conducted, where the different attacks try to get access to objects, preliminarily processed by method of compression. Graphically this process can be illustrated by this way:

$$U_1 \longrightarrow a_i \xrightarrow{\rho} m_j \xleftarrow{\rho} U_2$$
$$\downarrow$$
$$o_f$$

where U_1 is a user, who uses an attack $a_i \subseteq A_{max}$ to get access to a object $o_f \subseteq O_{max}$, preliminarily processed with method of compression $m_j \subseteq M_{max}$ for a protection by an user U_2, as $i=1,\ldots,n$, $j=1,\ldots,k$, $f=1,\ldots,l$.

For each cell of the matrix $E_{(k,n)}$ a logical processing is made with result logical 0 or logical 1 by the so called function of truth: $I_x(B)\begin{cases}1, x \in B\\ 0, x \notin B\end{cases}$ for the attack and method: $I_a(a_1), I_a(a_2), \ldots, I_a(a_i), \ldots, I_a(a_n)$, $I_m(m_1), I_m(m_2), \ldots, I_m(m_j), \ldots, I_m(m_k)$ and in the corresponding cell of the matrix is filled out the result from the logical expression: $I_a(a_i) \wedge I_m(m_j)$ on the of the experiments, which were carried out. If the obtained result is 1 (possible) (*x=1*), then during the experiment the attack had gotten an access to the method ($A \xrightarrow{\rho} M$), otherwise with result 0 (impossible) (*x=0*), the attack did not have gotten an access to an object, processed with methods of compression. On the base of the obtained results the set *D* can be singled out, which include all attacks and methods, for which is completed the following condition: $\mathrm{I}_a\left(a_i\right) \wedge I_m\left(m_j\right) = 1$.

For each cell from the second matrix $Y_{(k,n)}$ the function of truth is produced on the base of expert assessments: $Y_x(K)\begin{cases}1, x \in K\\ 0, x \notin K\end{cases}$ for the attack and method: $Y_a(a_1), Y_a(a_2), \ldots, Y_a(a_i), \ldots, Y_a(a_n)$, $Y_m(m_1), Y_m(m_2), \ldots, Y_m(m_j), \ldots, Y_m(m_k)$. For each oriented graph $A \xrightarrow{\rho} M$ the result from the following logical expression $Y_a(a_i) \wedge Y_m(m_j)$ is filled out. If the obtained result is 1 (true) (*x=1*), then an attack *A* can get access to an object *O*, processed with method of compression *M* ($A \xrightarrow{\rho} M$), otherwise with result 0 (*x=0*), an attack *A* can not get an access to an object *O*, compressed with method *M*. From the obtained results the set *Y* can be singled out, which include all attacks and methods, the following logical expression is realized for: $Y_a(a_i) \wedge Y_m(m_j) = 1$.

Crossing the set *D* with *Y* ($D \bigcap Y$)the set of possible relations attack—method (Θ) can be singled out, where $\Theta = \left[I_a\left(a_i\right) \wedge I_m\left(m_j\right) \right] \wedge \left[Y_a\left(a_i\right) \wedge Y_m\left(m_j\right) \right] = 1$. On Figure 3 are graphically presented the obtained results for possible relations between attacks' groups and methods' groups. To achieve calculation expenses reducing and visualization improving is working only with groups.

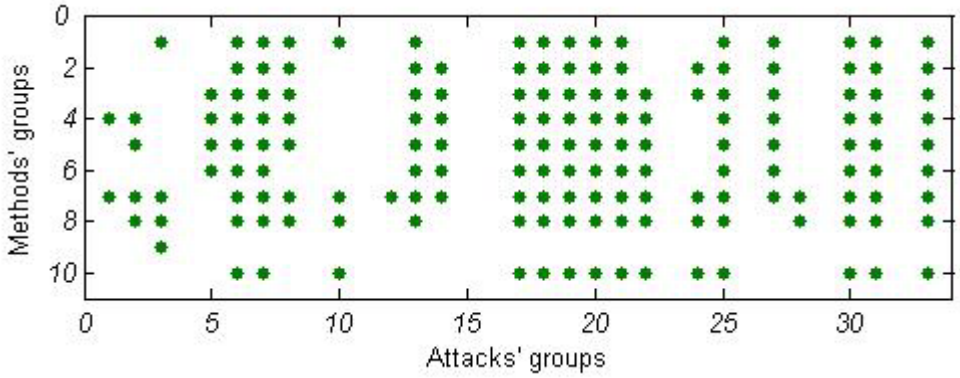

Figure 3 Possible relations between attacks' groups and methods' groups

2.2.) To determine the *REAL RELATIONS* between attacks, methods and objects.

Let the elements of the set Ω and Ξ form a totality of elements $\alpha \subseteq A$ then and then only, when for the elements $\omega_z \subseteq \Omega$ and $\xi_h \subseteq \Xi$ the following logical expression is realized for:

$$\mathrm{A} = \Omega \wedge \Xi = 1$$

The elements of the set Ω and Θ form a totality of elements $\beta \subseteq B$ then and then only, when for the elements $\omega_z \subseteq \Omega$ and $\theta_c \subseteq \Theta$ the following logical expression is realized for:

$$\mathrm{B} = \Omega \wedge \Theta = 1$$

The elements of the set Ξ and Θ form a totality of elements $\gamma \subseteq \Gamma$ then and then only, when for the elements $\xi_h \subseteq \Xi$ and $\theta_c \subseteq \Theta$ the following logical expression is realized for:

$$\Gamma = \Xi \wedge \Theta = 1$$

The set of all real relations between attacks, methods and objects, shown on Figure 4 (to achieve calculation expenses reducing and visualization improving is working only with groups), is $X = A \bigcap B \bigcap \Gamma$ or:

$$X = (\Omega \wedge \Xi) \wedge (\Omega \wedge \Theta) \wedge (\Xi \wedge \Theta) = A \wedge B \wedge \Gamma = 1$$

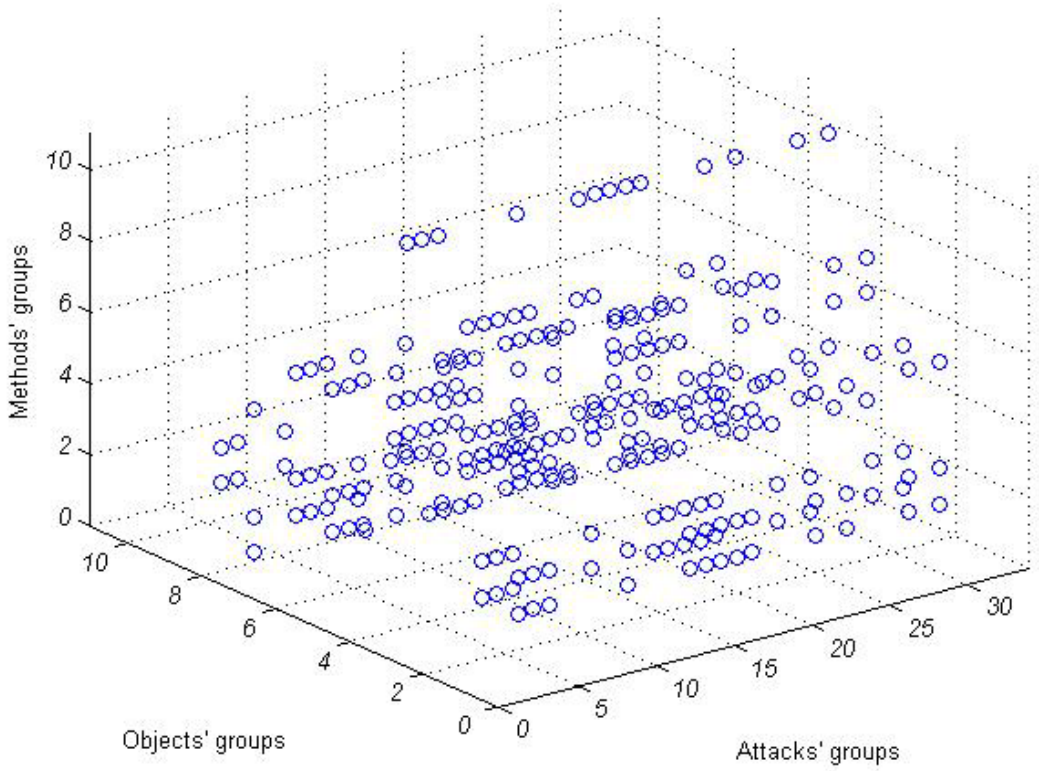

Figure 4 Real relations between attacks' groups, methods' groups and objects' groups

2.3.) To find the *POTENTIAL SETS* of attacks, methods and objects.

The set of potential attacks (A_{pot}) is expressed as *real* attacks (received from the real relations) in relation to the *maximum* number of attacks (A_{max}) and can be denoted as $A_{pot} = \{a_1, a_2, ..., a_i, ..., a_p\}$, where *p* is the index the *potential attacks* alter for, where $p \le n$.

The set of potential objects (O_{pot}) is expressed as *real* objects (received from the real relations) in relation to the *maximum* number of objects (O_{max}) and can be denoted as $O_{pot} = \{o_1, o_2, ..., o_f, ..., o_p\}$, where *p* is the index the *potential objects* alter for, where $p \le l$.

The set of potential methods (M_{pot}) is expressed as *real* methods (received from the real relations) in relation to the *maximum* number of methods (M_{max}) and can be denoted as $M_{pot} = \{m_1, m_2, ..., m_j, ..., m_p\}$, where *p* is the index the *potential methods* alter for, where $p \le k$.

Assessments

The following assessments could be made from the experiments which were carried out:

1) The selected number of maximum attacks' groups (33), methods' groups (10) and objects' groups (10) is sufficient for determining the potential sets.

2) The following general conclusions can be made after the experiments and expert assessments which were carried out:

- from totally 330 relations attack's group—method's group, after expert assessment 190 relations are singled out, proved by experiments are 191 relations and 160 *possible* relations attack's group—method's group are formed.
- from totally 100 relations method's group—object's group, after expert assessment 25 relations are singled out, proved by experiments are 25 relations and 19 *possible* relations method's group—object's group are formed.
- from totally 330 relations attack's group—method's group, after expert assessment 176 relations are singled out, proved by experiments are 201 relations and 161 *possible* relations attack's group—method's group are formed.

3) The combination of 489 440 *possible* relations among attacks' groups, methods' groups and objects' groups determines 269 *real* relations among the triple combination attack's group—method's group—object's group.

4) The number of attacks', methods' and objects' groups, which take part in the determination of the *potential sets* of attacks, methods and objects, which will be used during the next investigations, are as follows: groups of A_{pot}=18, groups of M_{pot}=8 and groups of O_{pot}=7.

5) The assessment of the potential attacks, methods and objects shows that assumptions made during the investigation will not affect the reliability of the results. The selected number of potential sets is sufficient for reaching conclusions and making recommendations.

6) The chosen methodology for analyzing the relations attack-method-object by means of matrix transformations is effective and operative, and it contains the necessary potential for new deep analyses in this and another related areas.

Conclusion

The investigation demonstrates the significant viability of such analyses. There is a possibility of specific planning of safety procedures and safety policies for the different computers, systems and networks configurations. Conditions are created for precise planning of economic expenses, connected with a specific safety policy with a specific configuration of computer, system and network. Future investigations will offer the possibility for exact determination of the relations attack-object-method.

Bibliography

[1] http://ncs.nlcv.bas.bg/index_en.htm

[2] Brad Gilmer, File Interchange Handbook: For professional images, audio and metadata, Focal Press, 2004.

[3] http://www.filext.com/alphalist.php?extstart=%5EA

[4] David Salomon, Data Compression: The Complete Reference, Springer Verlag New York, Inc., 2004.

[5] Werner Damm, Bernhard Josko, Amir Pnueli, Angelika Votintseva, A Discrete-Time UML Semantics for Concurrency and Communication in Safety-Critical Applications, Science of Computer Programming, Vol. 55, 1-3/2005.

Authors' Information

Dimitrina Polimirova – PhD Student, Research Associate, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, e-mail: polimira@nlcv.bas.bg

Eugene Nickolov – Professor, DSc, PhD, Eng, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, e-mail: eugene@nlcv.bas.bg

Cecko Nikolov – PhD Student, Research Associate, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, e-mail: nikolov@nlcv.bas.bg